WE CLAIM:

1. A method of conveying data traffic through a node of a communications network, the method comprising the steps of:

   a) assigning a parameter respecting the data traffic in an ingress interface;

   b) conveying the data traffic and the respective parameter to an egress interface; and

   c) processing the data traffic in the egress interface using the parameter.

2. A method as claimed in claim 1, wherein the parameter comprises any one or more of: information identifying the ingress interface; information identifying a quality of service (QoS) of data traffic received by the ingress port; information identifying a DiffServ codepoint of data traffic received by the ingress port; and information identifying a source address of data traffic received by the ingress port.

3. A method as claimed in claim 2, wherein the step of assigning a parameter comprises a step of evaluating the data traffic to derive a value of the parameter.

4. A method as claimed in claim 3, wherein the step of evaluating the data traffic comprises a step of assigning a default value of the parameter.

5. A method as claimed in claim 4, further comprising the steps of:

a) evaluating one or more layer-specific headers of the data traffic; and

b) modifying the default value of the parameter based on the evaluation result.

6. A method as claimed in claim 5, wherein the parameter is a normalized parameter value obtained by successively evaluating each one of the one or more layer-specific headers in turn, and modifying the parameter value based on each successive evaluation result.

7. A method as claimed in claim 1, wherein the step of conveying the data traffic and the respective parameter comprises the steps of:

a) inserting the parameter into an intra-switch header; and

b) appending the intra-switch header to the data traffic.

8. A method as claimed in claim 7, wherein the step of processing the data traffic comprises stripping the intra-switch header from the data traffic.

9. A method as claimed in claim 7, wherein the step of conveying the data traffic and the respective parameter further comprises a step of conveying the data traffic through a multicast-capable switch fabric.

10. A method as claimed in claim 9, wherein the data traffic and the respective parameter are replicated

by the switch fabric to one or more egress interfaces of the node.

11. A method as claimed in claim 1, wherein the step of processing the data traffic in the egress interface comprises any one or more of: implementing a traffic policing function; forwarding the data traffic to one or more respective egress network ports associated with the egress interface; and applying a predetermined policy.

12. A method as claimed in claim 11, wherein the step of implementing the traffic policing function comprises:

a) detecting congestion of the egress interface; and

b) discarding low-priority traffic such that the congestion is reduced.

13. A method as claimed in claim 11, wherein the policy is defined in respect of the egress interface.

14. A method as claimed in claim 11, wherein the policy is defined in respect of an egress network port associated with the egress interface.

15. A method as claimed in claim 11, wherein the policy comprises any one or more of: PASS; DROP; and TRANSLATE.

16. A method as claimed in claim 15, wherein the PASS policy is adapted to cause transmission of the data traffic from the node using a selected logical egress port associated with the egress interface.

17. A method as claimed in claim 15, wherein the DROP policy is adapted to prevent transmission of the data traffic from the node using a selected logical egress port associated with the egress interface.

18. A method as claimed in claim 15, wherein the TRANSLATE policy is adapted to modify one or more of a VLAN ID of the data traffic; a QoS parameter of the data traffic; and a DiffServ codepoint of the data traffic.

19. A method as claimed in claim 18, wherein the step of applying the TRANSLATE policy comprises the steps of:

a) querying a translation table; and

b) inserting the query result into the data traffic.

20. A method as claimed in claim 19, wherein the translation table comprises, for each parameter value, information identifying any one or more of: the VLAN ID; the QoS parameter; and the DiffServ codepoint.

21. A method as claimed in claim 19, wherein the translation table is specific to the egress interface.

22. A method as claimed in claim 19, wherein the translation table is specific to a logical egress port of the egress interface.

23. A node of a communications network, comprising:

a) an ingress interface adapted to assign a parameter respecting data traffic received over the network;

b) an egress interface adapted to process the data traffic using the parameter; and

c) means for conveying the data traffic and the respective parameter across the node between the ingress interface and the egress interface.

24. A node as claimed in claim 23, wherein the parameter comprises any one or more of: information identifying the ingress interface; information identifying a quality of service (QoS) of data traffic received by the ingress interface; information identifying a DiffServ codepoint (DSCP) of data traffic received by the ingress interface; and information identifying a source address of data traffic received by the ingress interface.

25. A node as claimed in claim 24, wherein the ingress interface comprises means for evaluating the data traffic to determine a value of the parameter.

26. A node as claimed in claim 25, wherein the means for evaluating the data traffic is adapted to assign a default value of the parameter.

27. A node as claimed in claim 26, wherein the means for evaluating the data traffic further comprises:

a) means for evaluating one or more layer-specific headers of the data traffic; and

b) means for modifying the default value of the parameter based on the evaluation result.

28. A node as claimed in claim 27, wherein the parameter is a normalized parameter value obtained by successively evaluating each one of the one or more layer-specific headers, and modifying the parameter value based on each successive evaluation result.

29. A node as claimed in claim 23, wherein the means for conveying the data traffic and the respective parameter comprises:

a) means for inserting the parameter into a header; and

b) means for appending the header to the data traffic.

30. A node as claimed in claim 29, wherein the header is stripped from the data traffic in the egress interface.

31. A node as claimed in claim 29, wherein the means for conveying the data traffic and the respective parameter further comprises a multicast-capable switch fabric.

32. A node as claimed in claim 31, wherein the multicast-capable switch network is adapted to replicate the data traffic and the respective parameter to one or more egress interfaces of the node.

33. A node as claimed in claim 23, wherein the egress interface comprises means for implementing a traffic policing function.

34. A node as claimed in claim 33, wherein the means for implementing the traffic policing function comprises:

a) means for detecting congestion of the egress interface; and

b) means for discarding low-priority traffic such that the congestion is reduced.

35. A node as claimed in claim 23, wherein the egress interface comprises means for forwarding the data traffic to one or more respective logical egress ports associated with the egress interface.

36. A node as claimed in claim 23, wherein the egress interface comprises means for applying a predetermined policy respecting the data traffic.

37. A node as claimed in claim 36, wherein the policy is specific to the egress interface.

38. A node as claimed in claim 36, wherein the policy is specific to a logical egress port associated with the egress interface.

39. A node as claimed in claim 36, wherein the policy comprises any one or more of: PASS; DROP; and TRANSLATE.

40. A node as claimed in claim 39, wherein the PASS policy is adapted to cause transmission of the data traffic from the node using a selected logical egress port associated with the egress interface.

41. A node as claimed in claim 39, wherein the DROP policy is adapted to prevent transmission of the data

traffic from the node using a selected logical egress port associated with the egress interface.

42. A node as claimed in claim 39, wherein the TRANSLATE policy is adapted to modify one or more of a VLAN ID of the data traffic; a QoS parameter of the data traffic; and a DiffServ codepoint of the data traffic.

43. A node as claimed in claim 42, wherein the means for applying the TRANSLATE policy comprises:

a) means for querying a translation table; and

b) means for inserting the query result into the data traffic.

44. A node as claimed in claim 43, wherein the translation table comprises, for each parameter value, information identifying any one or more of: the VLAN ID; the QoS parameter; and the DiffServ codepoint.

45. A node as claimed in claim 43, wherein the translation table is specific to the egress interface.

46. A node as claimed in claim 43, wherein the translation table is specific to a logical egress port of the egress interface.

47. An ingress interface of a network node, the ingress interface being adapted to receive inbound data traffic over a communications network, and comprising:

a) means for assigning a parameter respecting the data traffic received over the network; and

b) means for forwarding the data traffic and the respective parameter to an egress interface of the network node.

48. An ingress interface as claimed in claim 47, wherein the parameter comprises any one or more of: information identifying the ingress interface; information identifying a quality of service (QoS) of data traffic received by the ingress interface; information identifying a DiffServ codepoint (DSCP) of data traffic received by the ingress interface; and information identifying a source address of data traffic received by the ingress interface.

49. An ingress interface as claimed in claim 48, wherein the ingress interface comprises means for evaluating the data traffic to determine a value of the parameter.

50. An ingress interface as claimed in claim 49, wherein the means for evaluating the data traffic is adapted to assign a default value of the parameter.

51. An ingress interface as claimed in claim 50, wherein the means for evaluating the data traffic further comprises:

a) means for evaluating one or more layer-specific headers of the data traffic; and

b) means for modifying the default value of the parameter based on the evaluation result.

52. An ingress interface as claimed in claim 51, wherein the parameter is a normalized parameter value obtained by successively evaluating each one of the one or more layer-specific headers, and modifying the parameter value based on each successive evaluation result.

53. An ingress interface as claimed in claim 47, wherein the means for forwarding the data traffic and the respective parameter comprises:

a) means for inserting the parameter into an intra-switch header; and

b) means for appending the intra-switch header to the data traffic.

54. An egress interface of a network node, the egress interface being adapted to send outbound data traffic over a communications network, and comprising:

a) means for receiving data traffic and a respective parameter from an ingress interface of the node; and

b) means for processing the data traffic using the respective parameter.

55. An egress interface as claimed in claim 54, wherein the means for processing the data traffic comprises any one or more of:

a) means for implementing a traffic policing function;

b) means for forwarding the data traffic to one or more respective egress network ports associated with the egress interface; and

c) means for applying a predetermined policy respecting the data traffic.

56. An egress interface as claimed in claim 55, wherein the means for implementing the traffic policing function comprises:

a) means for detecting congestion of the egress interface; and

b) means for discarding low-priority traffic such that the congestion is reduced.

57. An egress interface as claimed in claim 55, wherein the policy is specific to the egress interface.

58. An egress interface as claimed in claim 55, wherein the policy is specific to a logical egress port associated with the egress interface.

59. An egress interface as claimed in claim 55, wherein the policy comprises any one or more of: PASS; DROP; and TRANSLATE.

60. An egress interface as claimed in claim 59, wherein the PASS policy is adapted to cause transmission of the data traffic from the node using a selected logical egress port associated with the egress interface.

61. An egress interface as claimed in claim 59, wherein the DROP policy is adapted to prevent transmission of the data traffic from the node using a selected logical egress port associated with the egress interface.

62. An egress interface as claimed in claim 59, wherein the TRANSLATE policy is adapted to modify one or more of a VLAN ID of the data traffic; a QoS parameter of the data traffic; and a DiffServ codepoint of the data traffic.

63. An egress interface as claimed in claim 62, wherein the means for applying the TRANSLATE policy comprises:

a) means for querying a translation table; and

b) means for inserting the query result into the data traffic.

64. An egress interface as claimed in claim 63, wherein the translation table comprises, for each parameter value, information identifying any one or more of: the VLAN ID; the QoS parameter; and the DiffServ codepoint.

65. An egress interface as claimed in claim 63, wherein the translation table is specific to the egress interface.

66. An egress interface as claimed in claim 63, wherein the translation table is specific to an egress network port of the egress interface.

67. A software program for controlling an ingress interface of a network node, the ingress interface being adapted to receive inbound data traffic over a communications network, the software program comprising:

a) software adapted to control the ingress interface to assign a parameter respecting the inbound data traffic; and

b) software adapted to control the ingress interface to forward the data traffic and the respective parameter to an egress interface of the network node.

68. A software program as claimed in claim 67, wherein the parameter comprises any one or more of: information identifying the ingress interface; information identifying a quality of service (QoS) of data traffic received by the ingress interface; information identifying a DiffServ codepoint (DSCP) of data traffic received by the ingress interface; and information identifying a source address of data traffic received by the ingress interface.

69. A software program as claimed in claim 68, further comprising software adapted to control the ingress interface to evaluate the data traffic to determine a value of the parameter.

70. A software program as claimed in claim 69, wherein the software adapted to control the ingress interface to evaluate the data traffic is adapted to control the ingress interface to assign a default value of the parameter.

71. A software program as claimed in claim 71, wherein the software adapted to control the ingress interface to evaluate the data traffic further comprises:

a) software adapted to evaluate one or more layer-specific headers of the data traffic; and

b) software adapted to modify the default value of the parameter based on the evaluation result.

72. A software program as claimed in claim 71, wherein the parameter is a normalized parameter value obtained by successively evaluating each one of the one or more layer-specific headers, and modifying the parameter value based on each successive evaluation result.

73. A software program as claimed in claim 67, wherein the software adapted to control the ingress interface to forward the data traffic and the respective parameter comprises:

a) software adapted to insert the parameter into an intra-switch header; and

b) software adapted to append the intra-switch header to the data traffic.

74. A software program for controlling an egress interface of a network node, the egress interface being adapted to send outbound data traffic over a communications network, the software program comprising software adapted to control the egress interface to process the data traffic using a respective parameter received from n ingress interface of the node.

75. A software program as claimed in claim 74, wherein the software adapted to control the egress interface

to process the data traffic comprises any one or more of:

a) software adapted to forward the data traffic to one or more respective egress network ports associated with the egress interface; and

b) software adapted to apply a predetermined policy respecting the data traffic.

76. A software program as claimed in claim 75, wherein the policy is specific to the egress interface.

77. A software program as claimed in claim 75, wherein the policy is specific to an egress network port associated with the egress interface.

78. A software program as claimed in claim 75, wherein the policy comprises any one or more of: PASS; DROP; and TRANSLATE.

79. A software program as claimed in claim 78, wherein the PASS policy is adapted to cause transmission of the data traffic from the node using a selected logical egress port associated with the egress interface.

80. A software program as claimed in claim 78, wherein the DROP policy is adapted to prevent transmission of the data traffic from the node using a selected egress network port associated with the egress interface.

81. A software program as claimed in claim 78, wherein the TRANSLATE policy is adapted to modify one or more

of a VLAN ID of the data traffic; a QoS parameter of the data traffic; and a DiffServ codepoint of the data traffic.

82. A software program as claimed in claim 81, wherein the software adapted to apply the TRANSLATE policy comprises:

a) software adapted to query a translation table; and

b) software adapted to insert the query result into the data traffic.

83. A software program as claimed in claim 82, wherein the translation table comprises, for each parameter value, information identifying any one or more of: the VLAN ID; the QoS parameter; and the DiffServ codepoint.

84. A software program as claimed in claim 82, wherein the translation table is specific to the egress interface.

85. A software program as claimed in claim 82, wherein the translation table is specific to an egress network port of the egress interface.